

STATEMENT
OF
OLIVER I. IRELAND
ON BEHALF OF
VISA U.S.A. INC.
BEFORE THE
SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION
OF THE
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

Securing Consumers' Data: Options Following Security Breaches

May 11, 2005

Good morning Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee. I am a partner in the law firm of Morrison & Foerster LLP, and practice in the firm's Washington, D.C. office. I am pleased to appear before the Subcommittee on behalf of the Visa, U.S.A. Inc., to discuss the important issue of consumer information security.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in developing and implementing technology, products, and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect Visa's members' cardholder information, thereby to protect the integrity of the Visa system.

Visa has substantial incentives to maintain strong security measures to protect cardholder information. The Visa system provides for zero liability to cardholders for unauthorized transactions. Cardholders are not responsible for unauthorized use of their cards. The Visa Zero Liability policy guarantees maximum protection for Visa cardholders against

fraud due to information security breaches. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs attributable to the harm and inconvenience that might be felt by cardholders or merchants. Accordingly, Visa aggressively protects the cardholder information of its members.

Existing Federal Laws and Rules for Information Security

Existing federal laws and regulations also obligate financial institutions to protect the personal information of their customers. Rules adopted under section 501(b) of the Gramm-Leach-Bliley Act of 1999 by the federal banking agencies and the Federal Trade Commission (“FTC”) (“GLBA 501(b) Rules”) establish information security standards for the financial institutions subject to the jurisdiction of these agencies. Under the GLBA 501(b) Rules, financial institutions must establish and maintain comprehensive information security programs to identify and assess the risks to customer information and then control these potential risks by adopting appropriate security measures.

Each financial institution’s program for information security must be risk-based. Every institution must tailor its program to the specific characteristics of its business, customer information and information systems, and must continuously assess the threats to its customer information and systems. As those threats change, the institution must appropriately adjust and upgrade its security measures to respond to those threats.

However, the scope of the GLBA 501(b) Rules is limited. Many holders of sensitive personal information are not financial institutions covered by the GLBA 501(b) Rules. For example, employers and most retail merchants are not covered by the GLBA 501(b) Rules, even though they may possess sensitive information about consumers.

Visa's Cardholder Information Security Plan

Because of its concerns about the adequacy of the security of information about Visa cardholders, Visa has developed and is implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("CISP"). CISP applies to all entities, including merchants, that store, process, transmit, or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers, or the Internet. CISP was developed to ensure that the cardholder information of Visa's members is kept protected and confidential. CISP includes not only data security standards but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

As a part of CISP, Visa requires all participating entities to comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include:

(1) install and maintain a working network firewall to protect data; (2) do not use vendor-supplied defaults for system passwords and security parameters; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) develop and maintain secure systems and applications; (7) restrict access to data on a "need-to-know" basis; (8) assign a unique ID to each person with computer access; (9) restrict physical access to data; (10) track all access to network resources and

data; (11) regularly test security systems and processes; and (12) implement and maintain an overall information security policy.

Payment Card Industry Data Security Standard

Visa is not the only credit card organization that has developed security standards. In order to avoid the potential for imposing conflicting requirements on merchants and others, in December of 2004, Visa, MasterCard, American Express, Discover, and Diners Club collaborated to align their respective data security requirements for merchants and third parties. Visa found that the differences between these security programs were more procedural than substantive. Therefore, Visa has been able to integrate CISP into a common set of data security requirements without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard (“PCI Standard”).

Neural Networks to Detect Fraud and Block Potentially Unauthorized Transactions

In addition to the CISP program, which helps to prevent the use of cardholder information for fraudulent purposes, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigation and card re-issuance. These

networks, coupled with CISP and Visa's Zero Liability, provide a high degree of protection from fraudulent credit card transactions to cardholders.

Expansion of Existing Requirements

Current protections notwithstanding, Visa believes that an obligation to protect sensitive personal information, similar to the GLBA 501(b) Rules, should apply broadly so that all businesses that maintain sensitive personal information will establish information security programs. Because consumer information knows no boundaries, it is critical that this obligation be uniform across all institutions in all jurisdictions.

Security Breach Notification

Closely related to the issue of information security is the question of what to do if a breach of that security occurs. Visa believes that where the breach creates a substantial risk of harm to consumers that the consumers can take action to prevent, the consumers should be notified about the breach so that they can take appropriate action to protect themselves. Both federal and California law already address this issue. California law currently requires notice to individuals of a breach of security involving their computerized personal information. The California law focuses on discrete types of information that are deemed to be sensitive personal information. The statute defines sensitive personal information as an individual's name plus any of the following: Social Security Number, driver's license number, California identification card number, or a financial account number, credit or debit card account number, in combination with any code that would permit access to the account. The California law includes an exception to the notification requirement when this personal information has been encrypted. The

California law only requires notice to be provided when personal information is “acquired by an unauthorized person.” Other states recently have enacted or are considering security breach notification laws; however, the details of some of the laws differ.

In March, the federal banking agencies issued final interagency guidance on response programs for unauthorized access to customer information and customer notice (“Guidance”). The Guidance applies to all financial institutions that are subject to banking agency GLBA 501(b) Rules and requires every covered institution that experiences a breach of security involving sensitive customer information to: (1) notify the institution’s primary federal regulator; (2) notify appropriate law enforcement authorities consistent with existing suspicious activity report rules; and (3) notify its affected customers where misuse of the information has occurred or is reasonably possible.

The keen interest that states have shown to legislate on the issue of security breach notification emphasizes the need for a single national standard for security breach notification in order to avoid confusion among consumers as to the significance of notices that they receive and among holders of information about consumers as to their notification responsibilities. In addition, any legislation on security breach notification should recognize compliance with the Guidance as compliance with any notification requirements.

Visa believes that a workable notification law that would require entities that maintain computerized sensitive personal information to notify individuals upon discovering a

significant breach of security of that data should be risk-based to avoid inundating consumers with notices where no action by consumers is required. As FTC Chairwoman Majoras recently testified to Congress, notices should be sent only if there is a “significant risk of harm,” because notices sent when there is not a significant risk of harm actually can cause individuals to overlook those notices that really are important.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.